UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | |
|---|---|
| SONAL BOSE, Individually, on Behalf of Herself and All Others Similarly Situated,<br><br>Plaintiffs,<br><br>v.<br><br>INTERCLICK, INC., a Delaware Corporation,<br><br>Defendant. | 10 Civ. 9183 (DAB)<br><br>**ORAL ARGUMENT REQUESTED** |

**DEFENDANT INTERCLICK, INC.'S MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS**

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Federal Cases



## State Cases

**Federal Statutes**



**Legislative History**



**State Statutes**



**Rules**

## PRELIMINARY STATEMENT

In her Complaint, plaintiff Sonal Bose ("Plaintiff") speculates that defendant Interclick, Inc. ("Interclick" or "Defendant"), an Internet advertising company, may have engaged in Web advertising practices that Plaintiff was not aware of in order to determine what advertisements to display. Plaintiff does not know whether her computer was even subjected to such practices and pleads no cognizable injury. Indeed, the only result of the practices Plaintiff alleges would have been that if, for example, she had visited travel-related websites, then she allegedly would have been more likely to be shown a travel-related advertisement. Plaintiff tries to stretch federal statutes and state law far beyond their limits to manufacture a putative class action claim out of these allegations. The Court should dismiss the action because Plaintiff's conclusory allegations fail to plead facts sufficient to state any cognizable claim or any cognizable injury.

Nearly a decade ago, Judge Buchwald of this Court dismissed a group of consolidated putative class actions that, like this action, challenged an Internet advertiser's alleged use of technology that tracked a computer's browsing on the Internet. In that detailed and authoritative decision, the court dismissed plaintiffs' complaint (including claims under the very federal statutes at issue in this action) because plaintiff's "bare assertion[s]" and "implausible" theories failed to create a colorable claim. *In re DoubleClick Inc. Privacy Litigation* ("*DoubleClick*"), 154 F. Supp. 2d 497, 510 (S.D.N.Y. 2001). Since that decision, the United States Supreme Court has articulated the requirement to plead *facts* setting forth a *plausible* basis for relief in the *Twombly* and *Iqbal* decisions. Plaintiff's pleading manifestly fails this test.

Plaintiff generally alleges that Interclick used tracking technology to monitor Web browsing on the Internet, and speculates that her computer may have been subject to this practice. (Plaintiff's Complaint ("Complaint" or "Compl.") ¶¶ 45, 48.) On this basis, Plaintiff asserts claims under the same two federal statutes at issue in *DoubleClick* — the Computer Fraud

and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030 *et seq*., and the Federal Wiretap Act ("Wiretap Act"), which is Title I of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 *et seq.* The CFAA makes it unlawful to engage in unauthorized access to a computer, and provides a civil remedy to individuals who suffer economic damages aggregating at least $5,000 in value as a result of a single act of unauthorized access (for example, from identity theft). *DoubleClick*, 154 F. Supp. 2d at 519-20. The Wiretap Act regulates the "interception" of the "contents" of "communications." *Id.* at 514.

Plaintiff's Complaint fails to state a cognizable claim under the CFAA because Plaintiff's conclusory allegations of damage cannot satisfy the CFAA's $5,000 threshold requirement under *Iqbal* and *Twombly*. Plaintiff alleges no facts (as opposed to mere labels and conclusions) suggesting that Interclick's alleged use of tracking technology caused a single cent of economic damage, let alone sufficient damage to reach the $5,000 statutory threshold. Plaintiff does not even claim that she has suffered $5,000 in economic damages, and any such claim would be implausible given her *de minimis* factual allegations.

To the extent Plaintiff attempts to rely on damage to other people's computers, Plaintiff lacks standing to raise other people's damage and fails to plead facts alleging any such damage. Even beyond those fundamental deficiencies, the claim fails as a matter of law. In *DoubleClick*, in dismissing the CFAA challenge to tracking technology on the ground that the plaintiffs in the consolidated cases could not satisfy the $5,000 in economic damages threshold, Judge Buchwald rejected the notion that DoubleClick's placing and accessing of tracking software on different computers could plausibly be considered a "single act" meeting the statutory threshold. 154 F. Supp. 2d at 524. Here, too, Interclick's alleged use of tracking technology as to different computers cannot plausibly be alleged to constitute a "single act."

Even if Plaintiff had a factual basis for claiming that she was subject to tracking technologies by Interclick, Plaintiff's claim under the Wiretap Act fails for three independent reasons, each one of which provides sufficient grounds for dismissing Plaintiff's Complaint. First, under the Wiretap Act, "interception" is not unlawful if *one* of the parties to the communication consents to the interception. 18 U.S.C. § 2511(2)(d). In *DoubleClick*, Judge Buchwald dismissed the Wiretap Act claim pursuant to this express statutory exemption, holding that one of the parties to the communications, the websites that plaintiffs were communicating with, had "consented" to the "interception." *DoubleClick*, 154 F. Supp. 2d at 514. The same reasoning bars Plaintiff's Wiretap Act claim here.

Second, and even more fundamentally, Plaintiff's Wiretap Act claim should also be dismissed because Plaintiff fails to allege any acquisition by Interclick of the "contents" of an electronic communication, other than parroting the language of the statute. A claim under the Wiretap Act requires proof of the "acquisition of the *contents* of any … electronic … communication." 18 U.S.C. § 2510(4) (emphasis added). The "contents" of a communication are "the substance, purport or meaning of that communication," 18 U.S.C. § 2510(8), not the "identity of the parties or the existence of the communication," S. Rep. No. 99-541, at 13 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3567. Plaintiff's own allegations, and the documentary evidence she incorporates by reference in her Complaint, each demonstrate that she fails to plead any facts showing that the alleged tracking technology at issue acquired the "contents" of any electronic communications, as defined under the Wiretap Act.

Third, the conduct alleged does not involve an "interception." Under the Wiretap Act, an "interception" occurs only when a communication is acquired during transmission, i.e., while it is in transit. Even taking Plaintiff's conclusory allegations as true, the alleged technology only

reviewed whether Plaintiff had previously visited websites. That is not "interception" under the Wiretap Act.

Accordingly, Plaintiff's CFAA and Wiretap Act claims should be dismissed with prejudice, and the Court should dismiss Plaintiff's state law claims for lack of supplemental jurisdiction. In the alternative, if the Court were to retain jurisdiction over Plaintiff's state law claims, they too should be dismissed because Plaintiff fails to allege facts sufficient to state a cognizable claim under any theory for the reasons set forth below.

## ALLEGATIONS OF THE COMPLAINT

The following statement is taken from the allegations of facts pleaded in the Complaint. These speculative allegations are taken as true solely for purposes of this motion to dismiss.

### Internet Advertising and Ad Networks

Many websites display third-party advertisements. (Compl. ¶¶ 10-12.) The publishers of websites sell advertising display space on those sites directly to advertisers or to intermediaries who operate "ad networks." (Compl. ¶¶ 12-13.) Interclick operates one such ad network. (Compl. ¶ 12.)

When a person uses the web browser of a computer to "visit" a website that has sold display space to an ad network operator, the website "causes" the user's browser "to communicate with the ad network's systems," which then display an advertisement that appears on the website page. (Compl. ¶ 11.) The ad network operator's object is to display an advertisement of interest to the computer user, potentially taking in account websites previously visited by the computer user. (Compl. ¶ 18.)

Interclick's "ad network" consists of websites from which Interclick has purchased advertisement display space. (Compl. ¶ 12.) Interclick's clients are advertisers and ad agencies

that pay Interclick fees for displaying their advertisements on the websites that make up this ad network. (Compl. ¶¶ 11-12.)

**Browser Cookies**

Many "online, third-party services" utilize "browser cookies," consisting of computer software code, to gather information about computer user Internet habits. (Compl. ¶ 18.) Plaintiff identifies a number of salient features of browser cookies:

- Third-parties deposit cookies on the Internet browsers of users' computers;
- Browser cookies contain unique identifiers, and while the cookies reside on a computer user's browser they collect "browsing history information" from the particular computer;
- The third-parties that deposit the browser cookies can access the cookies and the "browsing history information" stored on the cookies;
- Ad networks, like Interclick, use the browsing history information they collect from browser cookies to create "behavioral profiles" for particular computers; and
- When a computer that an ad agency has profiled using browser cookies visits a Web page on which the ad network serves advertisements, the computer systems of the ad agency use the profile to select particular categories of advertisements to be displayed to that computer.

(Compl. ¶ 18.)

**Flash Cookies**

Plaintiff alleges that Interclick used "flash cookies" (also known as local shared objects or "LSOs") "as a substitute and back-up for browser cookies." (Compl. ¶ 26.) Plaintiff alleges that when Interclick placed a standard browser cookie on a user's computer, it would also place an identical flash cookie. (Compl. ¶ 27.) If "the user deleted the browser cookies, the LSO [or

flash cookie] would be used to 're-spawn' the browser cookie" without notice to the user and without the user's consent. (*Id.*) Plaintiff relies upon and incorporates by reference an academic article on flash cookies. (Compl. ¶ 27) (citing "Flash Cookies and Privacy," A. Soltani, S. Canty. Q. Mayo, L. Thomas, C.J. Hoofnagle, U. Cal. Berkeley, Aug. 10, 2009, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id+1446862 (last accessed by Plaintiff Dec. 6, 2010)). As to Interclick, the article claims only that the researchers found that Interclick "respawned" a browser cookie by means of a flash cookie. Flash Cookies and Privacy, at 3. No other Interclick activity is identified in the article on which Plaintiff bases her claims or is otherwise alleged in the Complaint.

**"Browser Sniffing"**

According to Plaintiff, Interclick engaged in a practice that she refers to as "browser sniffing" "to determine whether a consumer had previously visited certain web pages." (Compl. ¶ 34.) Plaintiff alleges: "(a) in its code to display an advertisement to a consumer, Interclick embedded history-sniffing code invisible to the consumer; (b) the history-sniffing code contained a list of Web page hyperlinks; (c) although the hyperlinks were not displayed to the consumer, the consumer's browser automatically assigned each link a color designation based on whether the user had previously visited the Web page associated with the link; (d) the history-sniffing code performed an examination of the list of color-designated hyperlinks; (e) the history-sniffing code transmitted the results of this examination to Interclick's servers." (Compl. ¶ 35.) The Complaint challenges this alleged "browser sniffing."

**Plaintiff's "Experience" With Flash Cookies and "Browser Sniffing"**

Plaintiff alleges that she is a New York City resident (Compl. ¶ 4), but very little else about herself. While the Complaint includes a section entitled "Plaintiff's Experience" (¶¶ 44-

53), the allegations about Plaintiff's "experience" with Interclick's alleged tracking technology are minimal and speculative, and confirm that Plaintiff does not know whether *her* computer was even subject to "browser sniffing" or what function, if any, a flash cookie performed on *her* computer. Not surprisingly, Plaintiff fails to plead any facts suggesting any cognizable injury to herself or her computer.

Plaintiff alleges that "[o]n or about late October 2010," she examined the contents of her computer and discovered an LSO (or "flash cookie") allegedly "set by *interclick.com*." (Compl. ¶ 44.) Plaintiff alleges her "belief" that the flash cookie was part of Interclick's tracking technology. (Compl. ¶ 45.) Plaintiff does not allege whether the alleged flash cookie "respawned" a browser cookie on her computer. Plaintiff does not allege how the alleged flash cookie in any way interfered with or damaged her computer (nor could she).

Plaintiff's allegations regarding "browser sniffing" are similarly speculative. The Complaint alleges that "[b]ased on reports of Interclick's browser-history sniffing activities, Interclick's role as a major online ad network, and the presence of an interclick.com LSO on her computer, Plaintiff *believes* her web-browsing has been the [sic] subjected to Interclick's browser-history sniffing." (Compl. ¶ 48) (emphasis added). Plaintiff does not allege that the "browser sniffing" (which she "believes" occurred) in any way interfered with or damaged her computer (nor can she).

## ARGUMENT

### MOTION TO DISMISS STANDARD

"To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is *plausible on its face*.'" *Aschcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009) (emphasis added) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "Facial plausibility" means that the plaintiff's factual pleadings "allow[] the

court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. A complaint that pleads facts that are "merely consistent with" a defendant's liability is not plausible. *Id*.

Conclusory allegations that the defendant violated the standards of law do not satisfy the need for plausible factual allegations. *Twombly*, 550 U.S. at 555 (holding that "courts are not bound to accept as true a legal conclusion couched as a factual allegation") (internal quotation marks omitted). "'[A] plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.'" *Nomination Di Antonio E Paolo Gensini, S.N.C. v. H.E.R. Accessories Ltd.*, No. 07 Civ. 6959 (DAB), 2010 WL 4968072, at *2 (S.D.N.Y. Dec. 6, 2010) (Batts, J.) (quoting *Twombly*, 550 U.S. at 555). Thus, a court will not draw inferences favorable to a plaintiff based on allegations without "factual content" and will dismiss under Rule 12(b)(6) a claim premised on conclusory allegations. *Id*. at *6 (citing *Iqbal*, 129 S. Ct. at 1949).

In ruling on a motion to dismiss under Rule 12(b)(6) a court may also consider any documents incorporated by reference in the complaint. *Nomination Di Antonio E Paolo Gensini, S.N.C.*, 2010 WL 4968072, at *2.

**POINT I**

**PLAINTIFF FAILS TO ALLEGE A VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT.**

As in *DoubleClick*, Plaintiff fails to state a claim under the CFAA (Count I) because the Complaint does not and cannot adequately allege facts satisfying the statutory requirement to plead $5,000 in real economic damages from a single act. Plaintiff's allegations of damage consist of mere labels and the formulaic recitation of statutory language, and thus fail to state a plausible basis for relief. *Twombly*, 550 U.S. at 555; *Iqbal*, 129 S. Ct. at 1950.

The CFAA allows for a limited private right of action under specified circumstances. 18 U.S.C. § 1030(g). As in *DoubleClick*, the sole provision of the CFAA (18 U.S.C. § 1030(a)(5)) invoked in the Complaint (Compl. ¶ 84) is actionable only if a violation has caused "loss to one or more persons during any one-year period … aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). *See Register.com. Inc. v. Verio, Inc.*, 356 F.3d 393, 440 (2d Cir. 2004) (holding that "any civil action under CFAA involving 'damage or loss' .. must satisfy the $5,000 threshold" and reversing injunction based on the CFAA as record failed to demonstrate sufficient basis for claim of $5,000 in "*actual* damages or loss as a result of an alleged CFAA violation") (emphasis in original). Such damages "are limited to economic damages." 18 U.S.C. § 1030(g); *Register.com, Inc.*, 356 F.3d at 440.

Plaintiff fails to plead facts alleging that she sustained *any* real economic damages, let alone damages aggregating at least $5,000. The damage allegations of Count I (¶¶ 86-93) all merely parrot the words of the statute, contain purely conclusory allegations, and/or reference "damages" not cognizable under the CFAA. None of these paragraphs contain any allegation of *fact* establishing a plausible claim for $5,000 in cognizable damages. Under *Twombly* and *Iqbal*, mere labels and conclusions and "a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555; *Iqbal*, 129 S. Ct. at 1950; *see also Océ North America, Inc. v. MCS Services, Inc.*, No. WMN-10-CV-984, 2010 WL 3703277, at *5 (D. Md. Sept. 16, 2010) (granting Rule 12(b)(6) motion to dismiss CFAA claim because "Plaintiff's allegation that 'it has suffered impairment to the integrity or availability of its data, programs, systems, and information resulting in losses or damages in excess of $5000 during a one year period' is merely a conclusory statement and thus does not sufficiently plead the $5000 minimum damages requirement to bring a suit under the CFAA").

Plaintiff merely repeats the statutory language defining "impairment," "damage" and "loss" without stating any facts identifying any such harm to her computer. (Compl. ¶¶ 86, 87, 88, 89, 90, 92.) This is precisely the mere "formulaic recitation" rejected by *Twombly* and *Iqbal*. *Twombly*, 550 U.S. at 555; *Iqbal*, 129 S. Ct. at 1950.

Plaintiff also summarily asserts that she and putative class members have suffered "violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record." (Compl. ¶¶ 91, 93.) Devoid of factual allegations, this assertion also cannot sustain a cause of action under the CFAA. *Twombly*, 550 U.S. at 555; *Iqbal*, 129 S. Ct. at 1950. Moreover, loss of privacy and the supposed "economic value" of information about the Web habits of a user do not constitute real economic damage under the CFAA. As Judge Buchwald found in *DoubleClick*:

> A person who chooses to visit a Web page and is confronted by a targeted advertisement is no more deprived of his attention's economic value than are his offline peers. Similarly, although demographic information is valued highly . . ., the value of its collection has never been considered an economic loss to the subject. Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers.

*DoubleClick*, 154 F. Supp. 2d at 524; *see also AtPac v. Aptitude Solutions*, 730 F. Supp. 2d 1174, 1184-85 (E.D. Cal. 2010) (granting Rule 12(b)(6) motion to dismiss CFAA claim, noting that "courts interpreting the definition of 'loss' [under the CFAA] sufficient to bring a civil action have done so narrowly" and that allegation that "defendants 'obtained something of value exceeding $5000 in a single calendar year'" was insufficient to state claim under the CFAA). Indeed, Plaintiff implicitly appears to recognize that the allegations regarding "privacy" are not cognizable under the CFAA as she does not allege that such "loss" constitutes real economic damage nor does she cite any section of the statute supporting such a claim.

Because Plaintiff alleges no cognizable losses she has suffered, she invokes the provision of the CFAA referring to aggregating damages to more than one person during a one-year period. (Compl. ¶ 92.) However, this provision cannot save Plaintiff's pleading. First, economic damages under the CFAA "may only be aggregated across victims and over time for a *single* act." *DoubleClick*, 154 F. Supp. 2d at 523 (emphasis added). Plaintiff acknowledges this statutory requirement, as she makes the conclusory allegation that all of the alleged acts and omissions set forth in the Complaint are "an organized campaign of deployment" that "constituted a single act." (Compl. ¶ 64.) Not surprisingly, Plaintiff pleads no facts that make remotely plausible her sweeping claim that all of the deployment of either of the alleged tracking technologies alluded to in the Complaint, involving different websites and different computer users, can somehow constitute a "single act." Plaintiff's conception of a "single act" encompasses such disparate and separate phenomena that it has no analytical meaning whatsoever. Indeed, in *DoubleClick*, Judge Buchwald specifically held that DoubleClick's placing and accessing of tracking software on different computers could not be considered a "single act" for purposes of meeting the statutory threshold. 154 F. Supp. 2d at 524.

Second, at this point, prior to class certification (and a class could never be certified here, for numerous reasons), Plaintiff is the only plaintiff in this action and has no standing whatsoever to assert anyone's damages other than her own. *Thurmond v. Compaq Comp. Corp.*, 171 F. Supp. 2d 667, 680 (E.D. Tex. 2001) (plaintiff cannot rely upon damages allegedly suffered by absent putative class members to satisfy the CFAA $5,000 threshold). Plaintiff only asserts that the alleged "conduct has caused a loss to one or more persons…." (Compl. ¶ 92.) Accordingly, whether unidentified individuals absent from the Court could allege economic damage (and

Plaintiff makes no plausible allegation that they could) has no bearing on the sufficiency of Plaintiff's damages allegations.

Third, even if the alleged "damage" of absent putative class members somehow could satisfy the statutory requirements of the CFAA (and it cannot), Plaintiff's allegations merely recite the elements of a claim, and thus cannot satisfy the *Twombly* and *Iqbal* standard. (See Compl. ¶ 92.) No plausible real economic damage is alleged.

Accordingly, for all of these reasons, Plaintiff's CFAA claim should be dismissed.

## POINT II

## PLAINTIFF FAILS TO ALLEGE A VIOLATION OF THE WIRETAP ACT.

Plaintiff's Wiretap Act claim (Count II) should be dismissed under Rule 12(b)(6) for three independent reasons: (A) as in *DoubleClick*, there is no plausible allegation that website publishers contracting with Interclick had not "given prior consent"; (B) the alleged practices do not acquire the "contents" of a communication; and (C) the alleged practices do not constitute "interception." Plaintiff's separate allegations about (i) flash cookies and (ii) "browser sniffing" would each separately have to overcome all of these hurdles, but neither theory can overcome any of the hurdles.

The Wiretap Act prohibits a person from

> Intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor[ing] to intercept any wire, oral or electronic communication.

18 U.S.C. § 2511(1)(a).

The Wiretap Act defines "intercept" as

> the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device.

18 U.S.C. § 2510(4) (emphasis added).

Under the Wiretap Act, "contents"

> when used with respect to any wire, oral, or electronic communication, includes any information concerning *the substance, purport or meaning* of that communication.

18 U.S.C. § 2510(8) (emphasis added).

The Wiretap Act defines "electronic communication" as

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.

18 U.S.C. § 2510(12).

**A. There Is No Plausible Allegation That Any "Interception" Of Plaintiff's Electronic Communications Was Not With Prior Consent From Website Publishers.**

Section 2511(2)(d) of the Wiretap Act provides that "[i]t shall not be unlawful under this chapter for a person … to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given *prior consent* to such interception …." 18 U.S.C. § 2511(2)(d) (emphasis added).

Plaintiff is vague to the point of near opacity about which of her communications she believes that Interclick intercepted, with whom, and when. However, what Plaintiff does plead demonstrates that her Wiretap Act claim should be dismissed. Plaintiff only pleads one place of contact between Interclick and computer users such as herself — when a user visits a website on which Interclick serves an advertisement. (Compl. ¶ 18.) Thus, Plaintiff's claim relates to what the Complaint characterizes as communications between Plaintiff and the websites on which Interclick serves ads.

Plaintiff's allegations establish that (1) Interclick has an economic relationship with the websites because it pays them money for advertising space (Compl. ¶ 12); (2) the websites must be aware that Interclick uses tracking technology, including browser cookies, because that is

what ad networks like Interclick allegedly do — they deploy tracking technology to build profiles of users to better serve them advertisements (Compl. ¶ 18); and (3) the websites on which Interclick serves advertisements are not merely aware of or passively allowing interactions between Interclick and users, but instead the websites affirmatively *cause* users to communicate with Interclick's computer systems (Compl. ¶ 11).

These alleged facts demonstrate that the websites consented to any alleged interception of alleged communications between themselves and users, including Plaintiff. Based on the facts alleged, the websites would have known that Interclick was tracking users' web browsing history, and that the websites affirmatively directed the users to Interclick's systems, which allegedly place and download information from browser cookies.

Based on virtually identical facts, the court in *DoubleClick* dismissed the Wiretap Act claims. 154 F. Supp. 2d at 510, 514.[1] As here, plaintiffs in *DoubleClick* alleged that DoubleClick displayed ads on websites, and used tracking technology to intercept communications between users and those websites. Judge Buchwald held that given widespread knowledge of use of tracking technology by DoubleClick, "we find it implausible to infer that the Web sites had not authorized DoubleClick access" to the user communications. *Id*. at 510. The court rejected plaintiffs' bare assertion that the websites had not authorized the access. *Id*. Further, the court found it irrelevant that certain website operators might not have known of the precise technological means that DoubleClick used to intercept user communications. *Id*. All that is required under the Wiretap Act was that the websites approved of the access, not that they

[1] *DoubleClick*'s most detailed treatment of the "authorization/consent" issue is a section of the opinion addressing a claim under Title II of ECPA. However, while Title I (the Wiretap Act) uses the term "consent" and Title II uses the term "authorize," the court explains that the issue of consent and authorization are identical under Title I and II of ECPA, and accordingly dismissed the Title I claim as well. 154 F. Supp. 2d at 514.

understood the technological means by which DoubleClick went about performing the access. *Id*.

Similarly, here it is implausible to infer that the publishers of the websites on which Interclick had served ads did not consent. Plaintiff's mere assertion that Interclick's alleged conduct exceeded any authorization of the websites, is not, under *DoubleClick*, sufficient to defeat a motion to dismiss. *Id.*; (Compl. ¶¶ 50, 104.) Nor can a claim that the websites were not aware of flash cookies or "browser sniffing" save Plaintiff's Wiretap Act claim. All that matters, under *DoubleClick*, is that the website publisher was allegedly aware that Interclick was using tracking technology of some kind — the means used are irrelevant. 154 F. Supp. 2d at 510. Plaintiff's allegations establish that the websites must have been aware, at a minimum, that Interclick used some form of tracking technology. Thus, under *DoubleClick*, Plaintiff's Wiretap Act claim should be dismissed.

**B. The Wiretap Act Claim Should Be Dismissed Because Plaintiff's Allegations About Flash Cookies And "Browser Sniffing" Do Not Plead Facts Establishing The Acquisition Of The "Contents" Of A Communication.**

Plaintiff's Wiretap Act claim should also be dismissed because it fails to allege facts demonstrating that Interclick intercepted the "contents" of any electronic communications by Plaintiff.

The Wiretap Act (Title I of ECPA) addresses the *interception* of the *contents* of electronic communications during transmittal. *See, e.g., Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 556-57 (S.D.N.Y. 2008); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (Wiretap Act protects contents of communications, not the identity of the parties or the fact that the communications occurred).

Plaintiff has not alleged *facts* establishing that either the "flash cookie" she found on her computer, or the "browser sniffing" about which she speculates, acquired the *contents* of any

electronic communication. Plaintiff's only references to "contents" of electronic communication are in paragraphs 98, 101 and 102 of the Complaint, where Plaintiff merely parrots the language of the statute. As this Court has stated, "'a formulaic recitation of the elements of a cause of action will not do'" to state a claim upon which relief can be granted. *Nomination Di Antonio E Paolo Gensini, S.N.C.*, 2010 WL 4968072, at *2 (granting 12(b)(6) motion to dismiss; quoting *Twombly*, 550 U.S. at 555).

Thus, Plaintiff's allegations cannot support a Wiretap Act claim, as only the acquisition of the *contents* of a communication, not the identity of the parties or the fact that the communications occurred, is actionable under the statute. *See Jessup-Morgan*, 20 F. Supp. 2d at 1108 (granting Rule 12(b)(6) motion to dismiss because plaintiff alleged only that defendant disclosed identifying information, such as the author, about an electronic communication, and not the contents); *see also* S. Rep. No. 99-541, at 13 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3567 (the Wiretap Act "exclude[s] from the definition of the term 'contents,' the identity of the parties or the existence of the communication."); *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding that the Wiretap Act does not prohibit disclosure of non-content data, such as the number of times a video was viewed); *U.S. v. Parada*, 289 F. Supp. 2d 1291, 1304 (D. Kan. 2003) (holding that acquired phone numbers recorded on a cell phone were not "contents" of a communication under the Wiretap Act because "the contents would be the *substance* of the conversation") (emphasis added).

"Browser sniffing," at most, merely discloses that a browser previously visited a particular website. Plaintiff expressly alleges that "browser sniffing" "causes a user's previously visited *links to be displayed* in a different color than links a user has not visited." (Compl. ¶ 33) (emphasis added). Such information does not constitute the "contents" of a communication.

Further, Plaintiff does not allege any facts establishing that the alleged flash cookie she found on her computer did anything at all. Moreover, the article relied upon by Plaintiff and incorporated by reference in her Complaint (Compl. ¶ 27) states that the authors found that "Interclick respawned a HTTP cookie served by Reference.com" apparently by use of a flash cookie. Flash Cookies and Privacy, at 3. Nothing in the article states that Interclick used flash cookies to acquire the *contents* of communications (nor could it, given the technology), and Plaintiff alleges no additional facts to suggest that Defendants acquired the contents of any communication involving the Plaintiff.

**C. The Wiretap Act Claim Should Be Dismissed Because Flash Cookies And "Browser Sniffing" Do Not Cause "Interception."**

Plaintiff's Wiretap Act claim also should be dismissed for failure to plead "interception" of the contents of an electronic communication. Under the statute, the interception must occur contemporaneously with the transmittal of the communication, not after the fact. *See, e.g. Pure Power Boot Camp*, 587 F. Supp. 2d at 556-57 (surveying case law and holding that under the Wiretap Act an "'intercept … must occur contemporaneously with transmission'"). Plaintiff's factual allegations do not satisfy this requirement because she does not allege contemporaneous interception.

"Browser sniffing," as Plaintiff expressly alleges, does not involve the interception of communications while they are being transmitted. Instead, "browser sniffing" software reviews a browser's *past* interactions with specific websites. (Compl. ¶ 33.) Thus, Plaintiff alternatively refers to it as "history sniffing." (*Id.*) History is not contemporaneous. Accordingly, "browser sniffing" cannot support a claim of "interception" under the Wiretap Act.

Further, Plaintiff has not alleged facts establishing that the Interclick flash cookie she allegedly found on her computer interacted with her communications in any way — much less

contemporaneously "intercepted" Plaintiff's electronic communications. As discussed, at most Plaintiff alleges, by incorporation of an academic article in her Complaint, that the flash cookie could have been used to recreate a deleted browser cookie. Thus, Plaintiff alleges no facts to support any plausible claim of "interception" under the Wiretap Act.

## POINT III

## THE COURT SHOULD DISMISS PLAINTIFF'S STATE LAW CLAIMS FOR LACK OF JURISDICTION.

If the Court dismisses the Wiretap Act and CFAA claims, the sole predicate for federal jurisdiction, the Court should not exercise supplemental jurisdiction over the state law claims in the Complaint. 28 U.S.C. § 1367(c)(3). *See DoubleClick*, 154 F. Supp. 2d at 526 (declining to exercise supplemental jurisdiction over state law claims). "[W]hen the federal law claims have dropped out of the lawsuit in its early stages and only state law claims remain, the federal court should decline the exercise of jurisdiction…." *Carnegie-Mellon Univ. v. Cohill*, 484 U.S. 343, 350 (1988). Thus, this Court should decline to exercise supplemental jurisdiction over the state law claims and should dismiss the remainder of the Complaint.

## POINT IV

## PLAINTIFF FAILS TO ALLEGE ANY NEW YORK STATE LAW CLAIM.

Plaintiff's Complaint asserts a hodgepodge of New York state law claims (Counts III-VI). Even if the Court were to exercise supplemental jurisdiction (and it should not as per Point III above), the state law claims are deficient and should be dismissed for the following reasons.

### A. Plaintiff Fails to State A Claim Under N.Y. General Business Law Section 349.

New York General Business Law Section 349 provides, in relevant part, that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." N.Y. G.B.L. § 349(a). To state a claim under

Section 349, plaintiff must allege facts supporting a claim (1) that the act or practice was consumer-oriented; (2) that the act or practice was *misleading* in a material respect; and (3) that the consumer suffered injury as a result of the deceptive act or practice. *See, e.g.*, *Stutman v. Chemical Bank*, 95 N.Y.2d 24, 29 (2000). Plaintiff's conclusory allegations fail to satisfy at least the second and third elements.

As to the second element, Plaintiff fails to allege actionable misleading conduct on the part of Interclick. Section 349 requires that "[w]hether a representation or an omission, the deceptive practice must be 'likely to mislead a reasonable consumer acting reasonably under the circumstances.'" *Stutman*, 95 N.Y.2d at 29 (quoting *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 85 N.Y.2d 20, 26 (1995)). A "'deceptive act[] or practice[]' under the statute is not the mere invention of a scheme or marketing strategy, but the actual misrepresentation or omission to a consumer." *Goshen v. Mutual Life Ins. Co.*, 98 N.Y.2d 314, 325 (2002); *see also Solomon v. Bell Atlantic Corp.*, 9 A.D.3d 49, 51, 777 N.Y.S.2d 50, 52 (1st Dep't 2004) (Section 349 requires that "defendant made misrepresentations or omissions").

Apart from the conclusory allegation that Interclick engaged in "deception" and "fraud," (Compl. ¶¶ 112-13), Plaintiff fails to identify any misleading representation or omission by Interclick to Plaintiff, as required under Section 349. Plaintiff alleges only acts by Interclick of which Plaintiff was completely unaware while they were occurring, and which thus could not have deceived her. Indeed, Plaintiff does not even allege that she was aware of Interclick at the time of the alleged conduct.

Plaintiff also fails to satisfy the third element of Section 349 because she has not pleaded injury "by reason of" any alleged deception nor cognizable "actual damages." N.Y. G.B.L. § 349(h). First, Plaintiff does not allege that Interclick made any representations or omissions

that caused her harm. *See, e.g.*, *Oswego Laborers'*, 85 N.Y.2d at 26 (causation of harm required); *Solomon*, 9 A.D.3d at 51, 777 N.Y.S.2d at 52 (Section 349 requires "that the plaintiff was deceived by those misrepresentations or omissions and that as a result the plaintiff suffered injury"). In *Gale v. International Business Machines Corp.*, 9 A.D.3d 446, 447, 781 N.Y.S.2d 45, 47 (2d Dep't 2004), for example, the Appellate Division held that the plaintiff had failed to state a GBL Section 349 claim because he had failed to allege that he had seen any of the alleged deceptive statements made by the defendant. Similarly, here, Plaintiff identifies no deceptive statement or omission by Interclick that *caused* Plaintiff any injury. Plaintiff's alleged harm did not flow from any statement or omission by Interclick directed at Plaintiff, but instead whatever harm Plaintiff theoretically could have suffered resulted from acts of which she was completely unaware.

Second, Plaintiff alleges no "actual" harm as result of any alleged deceptive act. *Stutman*, 95 N.Y.2d at 29 (GBL § 349 requires showing of "actual" harm). As with her CFAA claim, Plaintiff's conclusory allegations (Compl. ¶¶ 116-17) fail to plead *facts* demonstrating any cognizable actual harm. Indeed, Plaintiff does not even know whether she was subject to "respawning" of browser cookies or "browser sniffing."

**B. Plaintiff Fails To State A Claim For Trespass to Personal Property/Chattels.**

In order to state a claim for trespass to chattels (or personal property) under New York law, Plaintiff must plead facts plausibly showing that Interclick "'intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in [Plaintiff's] possession,' and that [Plaintiff was] thereby harmed." *In re Jetblue Airways Corp. Privacy Litig.* ("*Jetblue*"), 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) (quoting *School of Visual Arts v. Kuprewicz*, 3 Misc. 3d 278, 771 N.Y.S.2d 804, 807 (N.Y. Sup. Ct. 2003)); *see also Register.com, Inc.*, 356 F.3d at 404 ("A trespass to a chattel may be committed by intentionally

… using or intermeddling with a chattel in the possession of another, where the chattel is impaired as to its condition, quality or value.") (citation omitted).

"Under New York law, liability only obtains on this cause of action if a defendant causes harm to 'the [owner's] materially valuable interest in the physical condition, quality, or value of the chattel, or if the [owner] is deprived of the use of the chattel for a substantial time.'" *Jetblue*, 379 F. Supp. 2d at 328 (quoting *School of Visual Arts*, 3 Misc. 3d at 281, 771 N.Y.S.2d at 807-08) (quoting Restatement (Second) of Torts § 218, com. e (1965)). Conclusory or generic allegations of harm are insufficient to state a claim. *Id.*; *see also Intel Corp. v. Hamadi*, 30 Cal. 4th 1342 (2003) (holding that tort of trespass to chattels did not encompass electronic communications that neither damaged the recipient computer system nor substantially impaired its functioning); *Hecht v. Components Int'l, Inc.*, 22 Misc. 3d 360, 370, 867 N.Y.S.2d 889, 899 (Sup. Ct. Nassau County 2008) ("Interference with information stored on a computer may give rise to trespass to chattel if plaintiff is dispossessed of the information or the information is impaired as to its condition, quality or value," but "[h]armless intermeddling with a chattel is not actionable" under New York law.).

Plaintiff makes only conclusory claims that Interclick's alleged trespass interfered with computers. (Compl. ¶¶ 122-28.) Plaintiff again pleads labels, but alleges no facts suggesting injury to her computer or dispossession of her computer. To the contrary, Plaintiff's few specific allegations demonstrate that any damages claim is implausible. Plaintiff alleges only that she found a flash cookie allegedly set by interlick.com when she examined the local storage associated with the Adobe Flash Player application on her computer. (Compl. ¶ 44.) There is no allegation, nor could there be, that this flash cookie harmed her computer, impaired its functioning or dispossessed her of its use.

As for "browser sniffing," Plaintiff does not even know if she was subject to the alleged practice. The Complaint does not allege any facts concerning the performance of her computer that she could attribute to the "browser sniffing" she believes may have occurred. None of the allegations of the Complaint establish that Plaintiff's use of her computer was impaired or that her computer was harmed. Indeed, "browser sniffing" by definition could cause no harm to a computer.

Accordingly, Plaintiff's claim for trespass should be dismissed. *See, e.g.*, *Elektra Entertainment Group, Inc. v. Santangelo*, No. 06 Civ. 11520, 2008 WL 4452393, at *7 (S.D.N.Y. Oct. 1, 2008) (dismissing trespass to chattels claim based on alleged unauthorized access to computer because, in part, plaintiff failed adequately to allege "actual injury either in the form of 'harm to the condition, quality or material value' of the computer, … or that they were deprived of the use of the computer for a substantial period of time"); *Jetblue*, 379 F. Supp. 2d at 328-29 (dismissing because "plaintiffs have not established that they suffered the type of harm that may be redressed through a claim for trespass to chattels" where "plaintiffs allege rather generically that they have suffered 'actual damages,'" "an irreparable injury for which there is no adequate remedy at law" and "harm to their privacy interests" and do not "allege any facts that could sustain … a showing" of the type of harm required).

**C. Plaintiff Fails To State A Claim For Breach Of Implied Contract Or For Unjust Enrichment.**

Although pleaded separately, Plaintiff's implied contract and unjust enrichment claims are duplicative and deficient. "Under New York law, the cause of action for unjust enrichment falls under the umbrella of quasi-contract or contract implied in law." *Jetblue*, 379 F. Supp. 2d at 329. In order to recover under this theory, Plaintiff must establish (1) the performance of services in good faith, (2) the acceptance of the services by the person to whom they are

rendered, (3) an expectation of compensation, and (4) the reasonable value of the services. *See Tower Int'l Inc. v. Caledonian Airways*, 969 F. Supp. 135, 138 (E.D.N.Y. 1997) (citing *Long v. Shore & Reich, Ltd.*, 25 F.3d 94, 98 (2d Cir. 1994)). Plaintiff has not alleged facts remotely establishing an implied-in-law or quasi-contract between herself and Interclick. There was no performance of services or expectation of compensation.

The Complaint alleges tort-like behavior, to which the concept of quasi-contract is inapplicable. A quasi-contract claim requires proof of a legally cognizable *relationship* between the parties. *See Jetblue*, 379 F. Supp. 2d at 329 (dismissing unjust enrichment claim against defendants as to whom plaintiffs "do not allege any facts to support a finding of 'direct dealings or an actual, substantive relationship'" with plaintiffs). Here, there was nothing that resembles "direct dealings or an actual, substantive relationship" between Plaintiff and Interclick, as Plaintiff does not even allege that Plaintiff and Interclick were aware of each other's existence.

In addition, Plaintiff fails to allege facts establishing that information that Interclick allegedly may have collected through the use of "browser sniffing" and flash cookies had economic value sufficient to support a claim for unjust enrichment. In *DoubleClick*, the court held that the uncompensated loss of "demographic information" collected by browser cookies cannot constitute "unjust enrichment to collectors." 154 F. Supp. 2d at 525.[2] Nothing in Plaintiff's Complaint suggests that the information supposedly collected was more extensive or somehow more valuable to Plaintiff than the information at issue in *DoubleClick*.

Accordingly, Plaintiff fails to state a claim for implied contract or unjust enrichment.

---

[2] The alleged "demographic information" at issue in *DoubleClick* included personal information that went well beyond anything that Plaintiff alleges in this case, including names, e-mail addresses, home and business addresses and telephone numbers. 154 F. Supp. 2d at 503.

## CONCLUSION

For the foregoing reasons, defendant Interclick, Inc. respectfully requests that the Court grant its Motion to Dismiss the Complaint with prejudice and that the Court grant such other and further relief for Defendant as the Court deems just and proper.

Dated: New York, New York
February 28, 2011

**RICHARD AND RICHARD, P.A.**

Dennis A. Richard (*pro hac vice* application pending)
Michael R. Tolley (*pro hac vice* application pending)
825 Brickell Bay Drive
Tower III, Suite 1748
Miami, Florida 33131
(305) 374-6688
(305) 374-0384 (fax)
dennis@richardandrichard.com
Michael@richardandrichard.com

*Attorneys for Defendant Interclick, Inc.*

**GREENBERG TRAURIG, LLP**

By: /S/ Stephen L. Saxl
Stephen L. Saxl
William A. Wargo
200 Park Avenue
New York, New York 10166
(212) 801-9200
(212) 801-6400 (fax)
saxls@gtlaw.com
wargow@gtlaw.com

Ian C. Ballon (*pro hac vice* application pending)
GREENBERG TRAURIG, LLP
2450 Colorado Avenue
Suite 400E
Santa Monica, CA 90404
(310) 586-7700
(310) 586-0575 (fax)
ballon@gtlaw.com

*Attorneys for Defendant Interclick, Inc.*